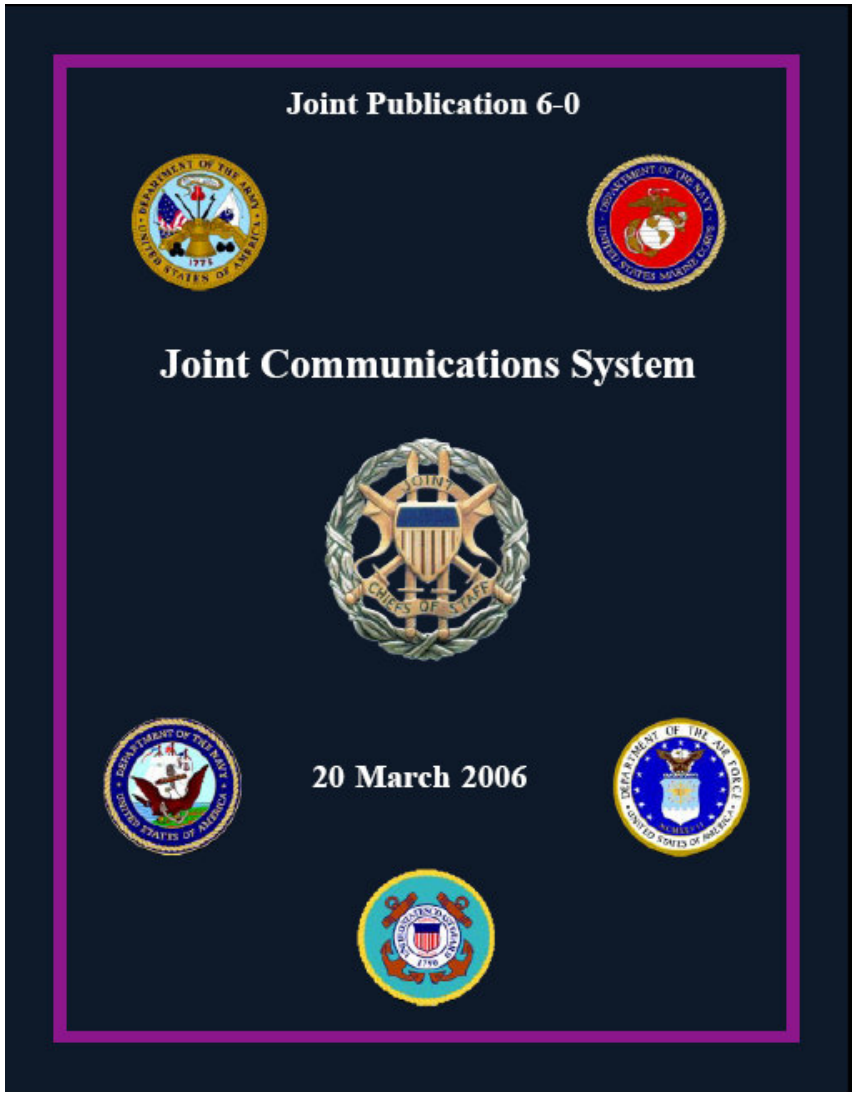
# Net-Centricity & Net-Ready:

## Beyond Technical Interoperability & C4ISR

**Jack Zavin**
**Associate Director**
**DoD CIO/A&I Directorate**
**(703) 607-0238**
**Jack.Zavin@osd.mil**

**SSTC 4 May 2006**

# C4 is now "Communications System"




SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 6-0
DATED 30 MAY 1995

- Consolidates Joint Publication (JP) 6-02, *Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer Systems* and JP 6-0 formerly called *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*
- Discontinues use of the term "command, control, communications, and computers (C4) systems" and replaces it with "communications system"
- Deconstructs the acronym "C4ISR" into its component parts: "command and control (C2)," "communications system," and "intelligence, surveillance, and reconnaissance (ISR)." Only the component being discussed is appropriately referenced.
- Discusses information superiority
- Introduces joint force network operations (NETOPS)
- Introduces network enabled operations
- Provides more information on satellite communications (SATCOM)
- Provides a communications system estimate guide

# Achieving Interoperability: A journey not a destination

***Interoperability is more than just the technical exchange of information:***
***Solutions Sets must cover Process, Organization, People, Information, and Materiel over the life cycle;***
***and it must be balanced with Information Assurance***

*Interoperability:*
*" The ability of systems, units or forces to provide services to and accept services from other systems, units or forces and use the services to enable them to operate effectively together."* *(JP 1-02 (emphasis added)*

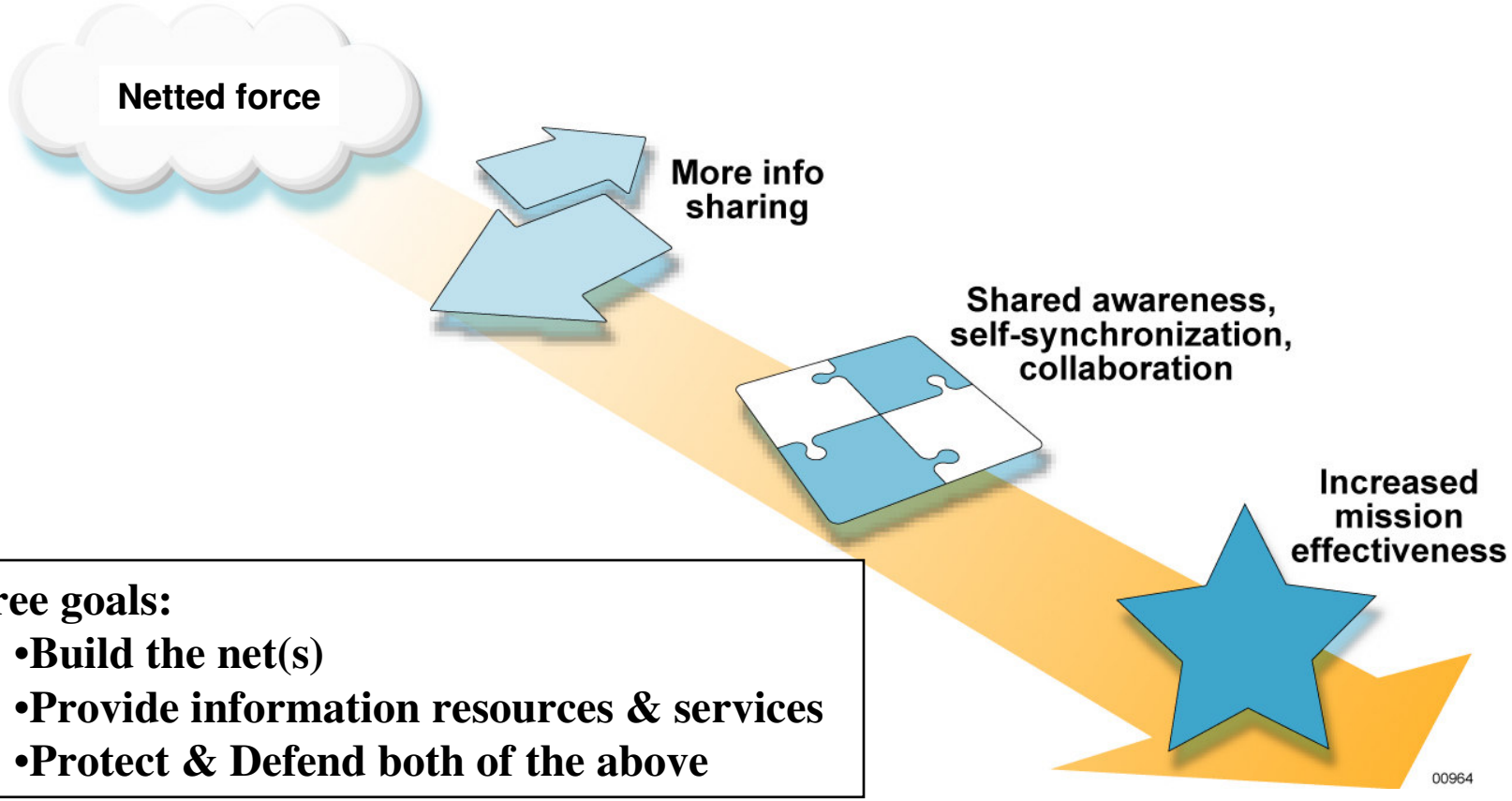
*Information Assurance:*
*"The ability to provide the measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." (CNSSI 4009)*

**References: DoDD 4630.5, May 5, 2004 & DoDI 4630.8 , 30 June 2004**

# Net-Centric Operations
# A Transformation Enabler

***Net-Centricity*** **is the empowerment of all users with the ability to easily discover, access, integrate, correlate and fuse data/information that support their mission objectives unconstrained by geospatial location or time of day .**

**Information Age Evolution** → **Net-Centric Operations and Warfare**




**Three goals:**

- **Build the net(s)**
- **Provide information resources & services**
- **Protect & Defend both of the above**

# Net-Centric Attributes

| Attribute | Description |
|---|---|
| Internet & World Wide Web Like | Adapting Internet & World WideWeb standards with additions as needed for mobility, surety, and military unique features. |
| Secure & available information transport | Encryption initially for core transport backbone; goal is edge to edge; hardened against denial of service |
| Quality of protection | Data/Information tagged by originator for classification & handling instructions. |
| Post in parallel | Information Producers make information visible and available at the earliest point of usability |
| Smart pull (vice smart push) | Users can find and pull directly, subscribe or use value added services (e.g. discovery). User Defined Operational Picture v Common Operational Picture |
| Information/Data centric | Data separate from applications and services. |
| Shared Applications & Services | Users can pull multiple apps to access same data or choose same applications (e.g., for collaboration). Applications on "desktop" or as a service |
| Trusted & Tailored Access | Access to the information transport, data/information, applications & services tied to user's role and identity. |
| Quality of service | Tailored for information form: voice, still imagery, video/moving imagery, data, and collaboration. Provide for precedence & preemption. |

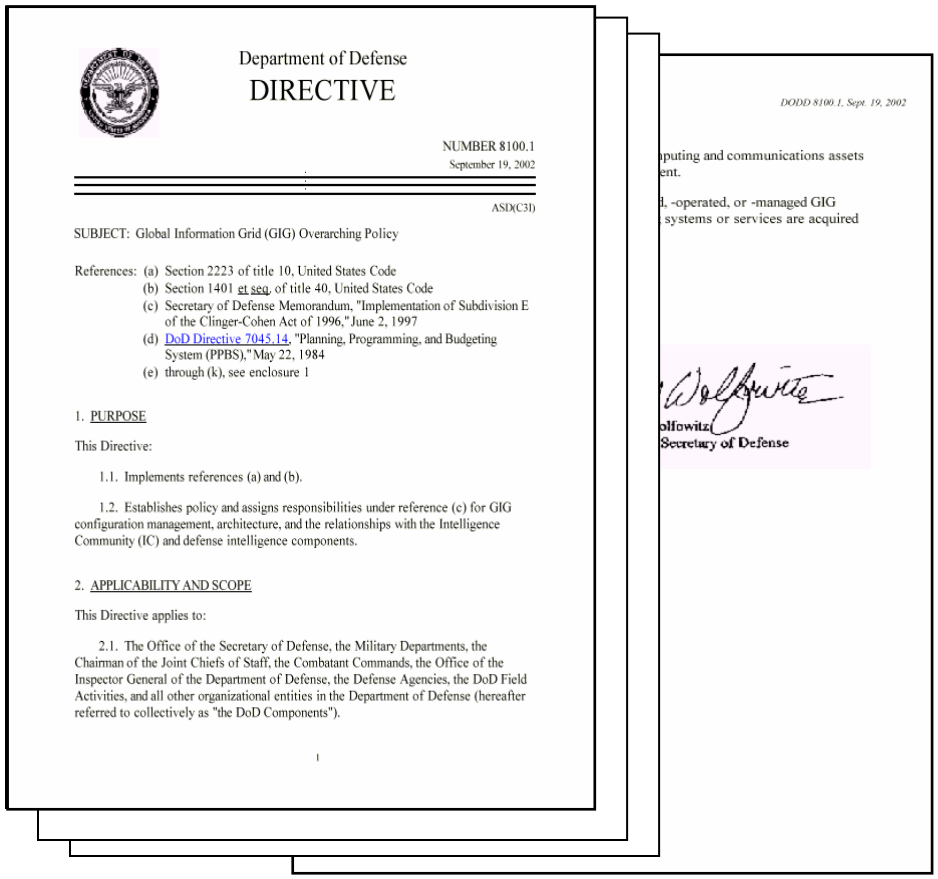
# DoD's Net-Centric Data Strategy

- **The Net-Centric Data Strategy (May 9, 2003 +) is a key enabler of the Department's transformation:**
- **The Strategy provides the foundation for managing the Department's data in a net-centric environment, including:**
  - ✓ **Ensuring data are visible, accessible, and understandable when needed and where needed**
  - ✓ **"Tagging" of all data (intelligence, non-intelligence, raw, and processed) with metadata to enable discovery by known and unanticipated users in the DoD**
  - ✓ **Posting of all data to shared spaces for users to access except when limited by security, policy, or regulations**
  - ✓ **Organizing around Communities of Interest (COIs) that are supported by Warfighter, Business, and Intelligence Domains.**

**+ DOD Directive 8320.2, December 2, 2004**

# The Global Information Grid

## DoD Directive 8100.1



Department of Defense
DIRECTIVE

NUMBER 8100.1
September 19, 2002

ASD(C3I)

SUBJECT: Global Information Grid (GIG) Overarching Policy

References: (a) Section 2223 of title 10, United States Code
(b) Section 1401 et seq. of title 40, United States Code
(c) Secretary of Defense Memorandum, "Implementation of Subdivision E of the Clinger-Cohen Act of 1996," June 2, 1997
(d) DoD Directive 7045.14, "Planning, Programming, and Budgeting System (PPBS)," May 22, 1984
(e) through (k), see enclosure 1

1. PURPOSE

This Directive:

1.1. Implements references (a) and (b).

1.2. Establishes policy and assigns responsibilities under reference (c) for GIG configuration management, architecture, and the relationships with the Intelligence Community (IC) and defense intelligence components.

2. APPLICABILITY AND SCOPE

This Directive applies to:

2.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as "the DoD Components").

1

DODD 8100.1, Sept. 19, 2002

puting and communications assets
ent.

l, -operated, or -managed GIG
systems or services are acquired

olfowitz
Secretary of Defense

**The GIG supports all Department of Defense, National Security and related Intelligence Community missions and functions, in war and in peace.**

**The GIG is the globally interconnected, end-to end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand by warfighters, policy makers and support personnel. It includes National Security Systems as defined in Title 40 USC.**

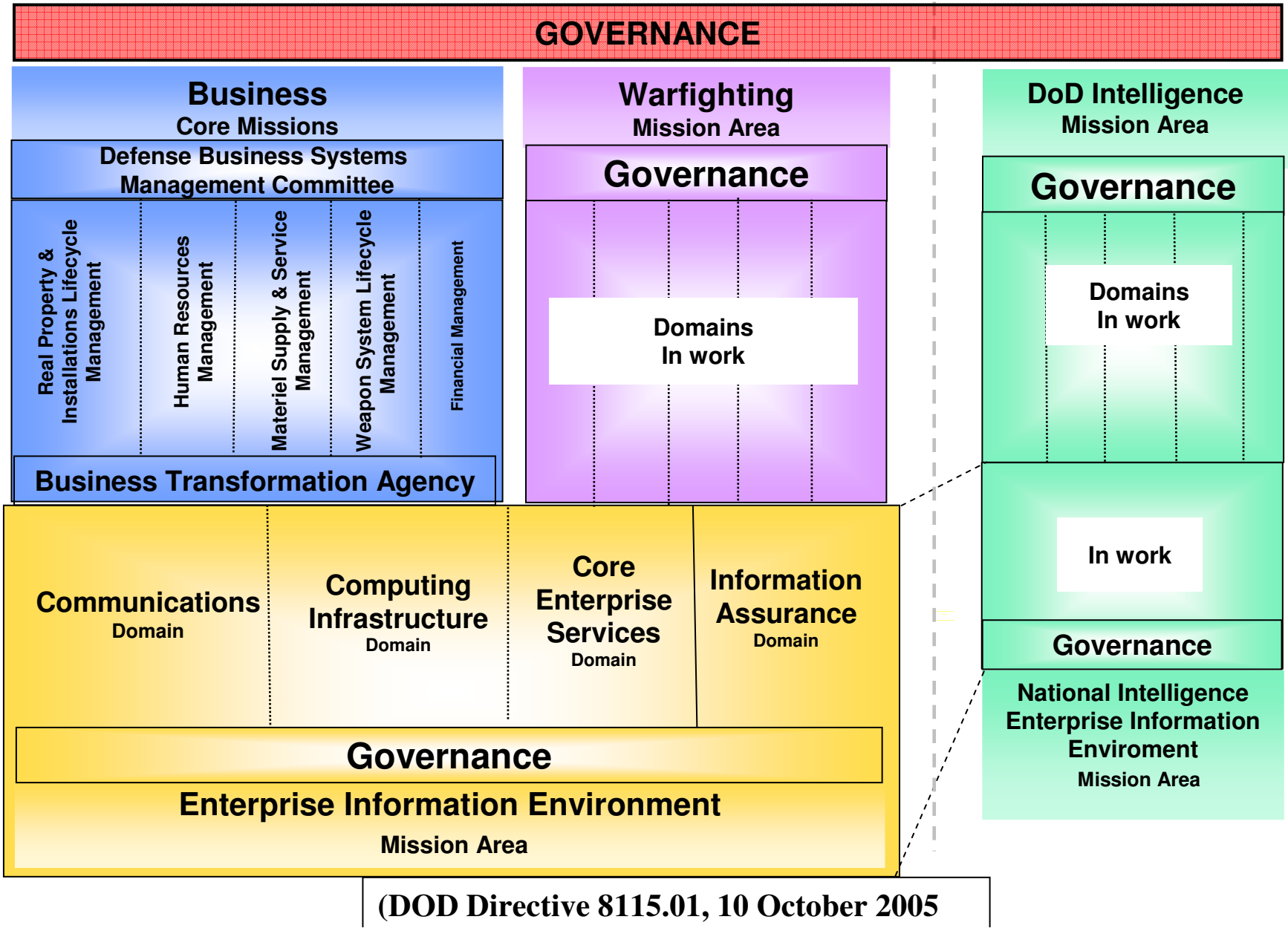
**The GIG includes all owned and leased communications and computing systems, and other associated services.**

**The GIG provides capabilities from all operating locations.**

**The GIG provides interfaces to coalition, allied, and non-DoD users and systems.**

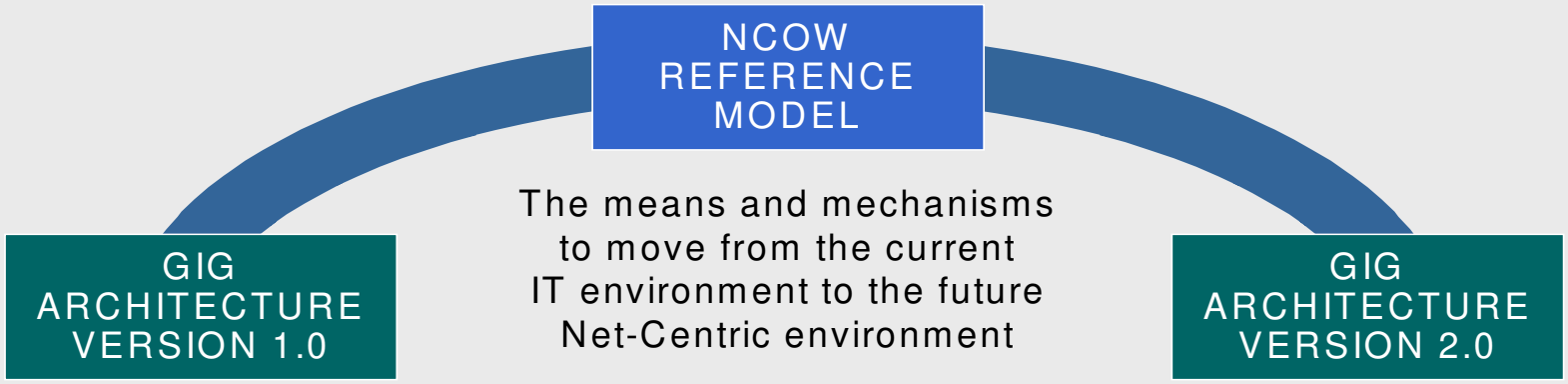
**The GIG is NOT – A Program, Box, or Network. It is an Organizing Construct & Architectural Framework for managing all of DoD's Information Capabilities**

# Global Information Grid
## Governance & Portfolios




(DOD Directive 8115.01, 10 October 2005

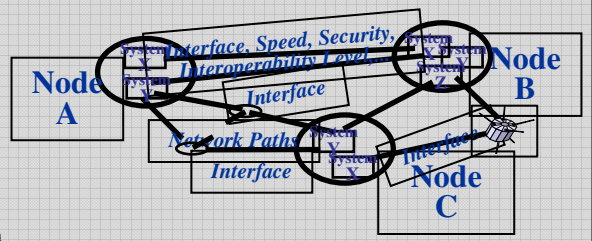
# Net-Centric Operations & Warfare Reference Model



# Integrated Architecture* In Context

**All View**

*Functional & Organizational*


***The Operational View*** **describes and interrelates the operational elements, tasks and activities, and information flows required to accomplish mission operations.**

***The Systems View*** **describes and interrelates the existing or postulated technologies, systems, and other resources intended to support the operational view.**

- Information Format & Content
- Information Processing
- Information Assurance
- Information Transfer
- User Interface

***The Technical Standards View*** **describes the profile of rules, standards, and conventions governing systems implementation.**

*"AS-IS" & "TO-BE(s)"*

*Non-Materiel Solutions*

**DoD Information Technology Standards Registry**

***as described in the DoD Architecture Framework DoDAF V 1.0**

**The bottom line: keep this equation balanced:OV = SV + Non-Materiel**

# Net-Ready Key Performance Parameter Attributes

**Information needs …**

**Information timeliness …**

**Information assurance …**

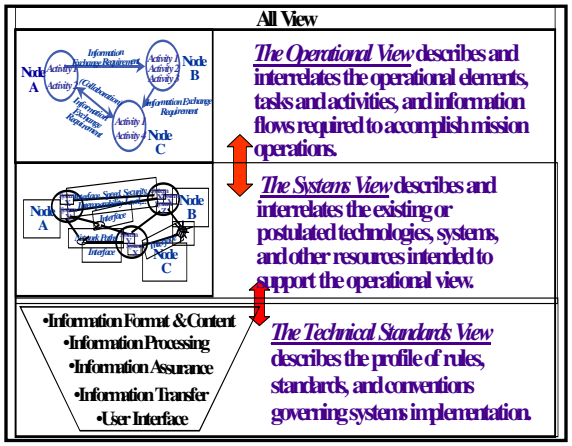
**Net-enabled …**

- ☑ **Information Needs: A condition or situation requiring knowledge or intelligence derived from received, stored, or processed data and information.**
- ☑ **Information Timeliness: Occurring at a suitable or appropriate time for a particular condition or situation.**
- ☑ **Information Assurance: Protecting and defending information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.**
- ☑ **Net-Enabled: The continuous ability to interface and interoperate to achieve operationally secure exchanges of information in conformance with enterprise constraints.**

**References: DoDD 4630.5, May 5, 2004 & DoDI 4630.8 , 30 June 2004**

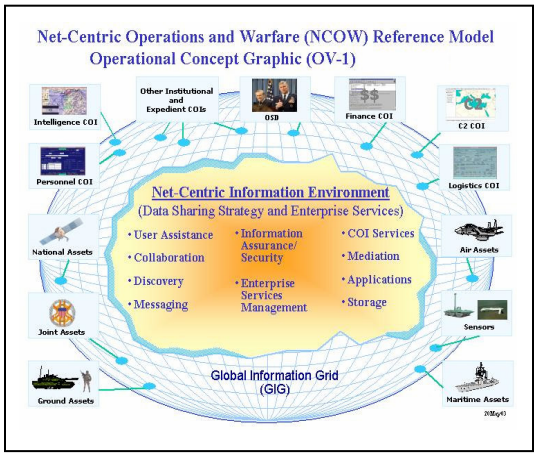
# Net-Ready Key Performance Parameter Components & Verification

## Supporting Integrated Architecture(s)



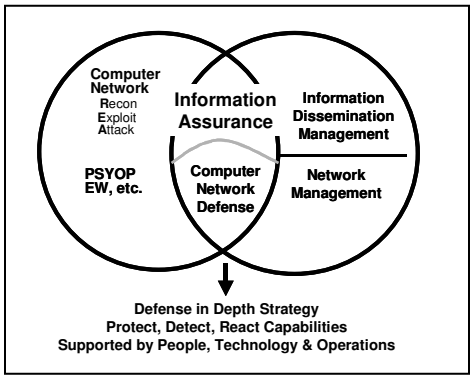

- Inspection
- Analysis
- Test

## NCOW RM Compliance




- Inspection
- Analysis

## IA Compliance




- Inspection
- Analysis

## Compliance With Applicable Key Interface Profiles

| | |
|---|---|
| | ***Communications KIPs*** |
| 1. | Logical Networks to DISN Transport Backbone |
| 2. | Space to Terrestrial Interface |
| 3. | JTRS Coalition |
| 4. | JTRS Component to JTF Headquarters |
| 5. | Teleport (i.e., deployed interface to DISN) |
| 6. | Joint Interconnection Service |
| 7. | DISN Service Delivery Node |
| 8. | Secure End-to-End Service Delivery Node (e.g., SCI/Collateral KIP) |
| | |
| | ***Computing KIPs*** |
| 9. | Application Server to Database Server |
| 10. | Client to Server |
| 11. | Applications to COE/CCP |
| | |
| | ***Network Operations KIPs*** |
| 12. | End System to PKI |
| 13. | Management Systems to (integrated) Management Systems |
| 14. | Management Systems to Managed Systems |
| 15. | IDM to Distribution Infrastructure |
| 16. | Information Servers to IDM Infrastructure |
| | |
| | ***Applications*** |
| 17. | Application Server to Shared Data - FICP(S/AD) |

- Inspection
- Test

**CJCSI 6212.01D, 8 March 2006**

# OEF/OIF Observations*

- Network Management
  - Network planning only at brigade level, not division.
  - Primarily used for situational awareness.
- **Meteorological Support Team**
  - Not used. Rather USAF weather info posted on SIPRNET.
- Topographic Support
  - Provides decision makers with the products required.
  - Operators cited difficulties in operating, transporting and maintaining the system.

** Extract from Briefing on ABCS in OEF/OIF, Dr. Hutchison, DOT&E, NDIA Interoperability 2004*

# Empowering Known and Unanticipated Users

Shift Power to the User:

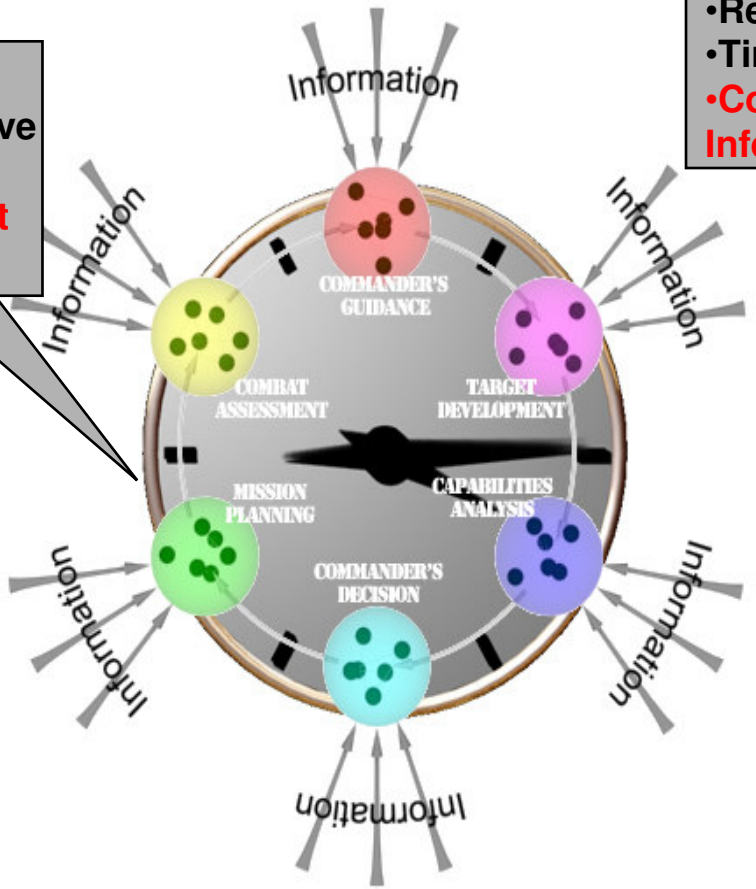
- Bring data consumers, producers, and system developers closer together through Communities Of Interest
- Guide data management activities through user-driven metrics, user ratings/feedback, and data sharing incentives
- Provide the infrastructure and services (e.g., GIG BE, NCES, Shared Spaces, Catalogs) to permit the user to find and retrieve data

***QUESTIONS ?***

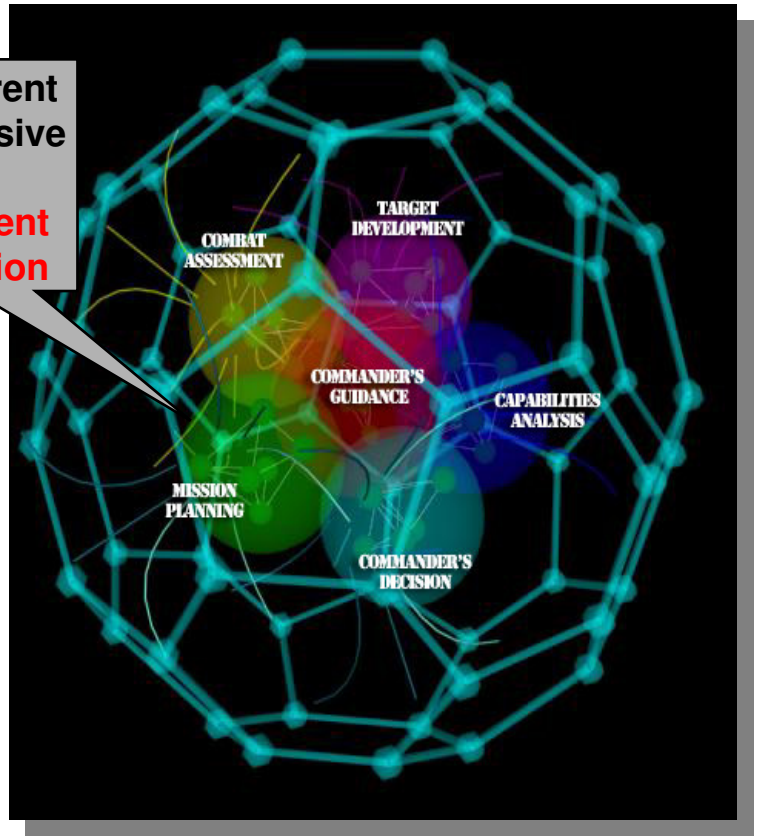
# The Joint Targeting Cycle in a Net-Centric Environment

"As Is"

•Sequential
•Unresponsive
•Untimely
•Inconsistent Information

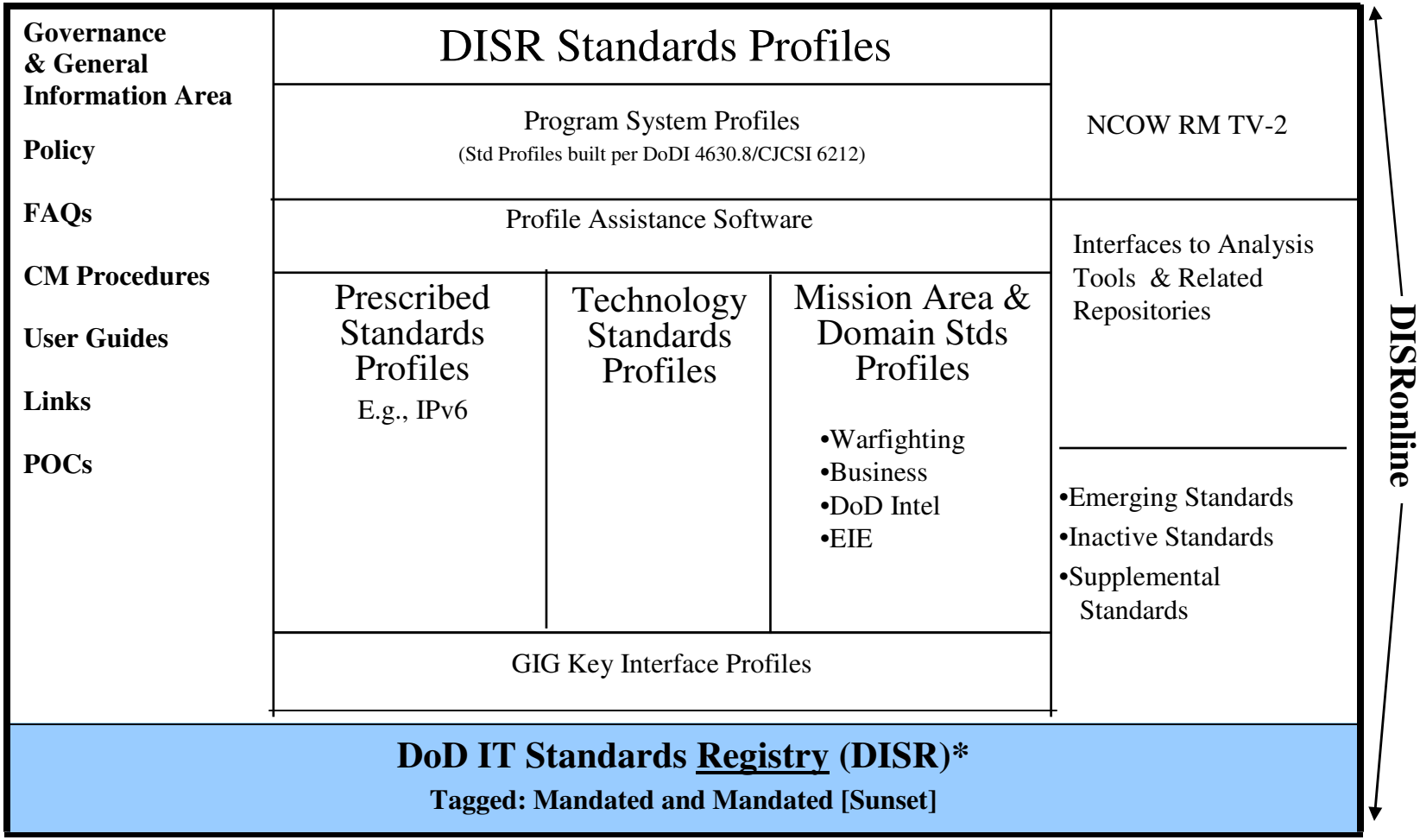



•Concurrent
•Responsive
•Timely
•Consistent Information




"To Be"

# DISR & DISRonline
# (The Net-Centric IT Standards Resources)




**The content of the Joint Technical Architecture*